```
File  8:Ei Compendex(R) 1970-2005/Jan W3
         (c) 2005 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2005/Jan
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Feb W2
         (c) 2005 BLDSC all rts. reserv.
File   2:INSPEC 1969-2005/Feb W1
         (c) 2005 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2005/Jan W1
         (c)2005 Japan Science and Tech Corp(JST)
File 483:Newspaper Abs Daily 1986-2005/Feb 14
         (c) 2005 ProQuest Info&Learning
File   6:NTIS 1964-2005/Feb W1
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2005/Feb W1
         (c) 2005 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Feb W2
         (c) 2005 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Jan
         (c) 2005 The HW Wilson Co.
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 266:FEDRIP 2004/Nov
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2005/Jan W2
         (c) 2005 FIZ TECHNIK
File 438:Library Lit. & Info. Science 1984-2005/Jan
         (c) 2005 The HW Wilson Co
File  62:SPIN(R) 1975-2005/Nov W4
         (c) 2005 American Institute of Physics
File 239:Mathsci 1940-2005/Mar
         (c) 2005 American Mathematical Society

Set     Items   Description
S1      13020   (SCALE? ? OR SCALABLE OR SCALING OR SCALABILITY OR PROGRES-
             SIV?)(3N)(ENCOD??? OR COD???) OR TRANSCOD???
S2        156   (SCALE? ? OR SCALABLE OR SCALING OR SCALABILITY OR PROGRES-
             SIV?)(3N)(ENCRYPT? OR ENCIPHER? OR ENCYPHER?)
S3       4913   (CIPHER OR CYPHER)()BLOCK()CHAIN??? OR CBC OR ICBC
S4         21   S1 AND S2:S3
S5         16   RD (unique items)
S6         86   S1 AND (ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR CIPHER? OR C-
             YPHER?)
S7         60   RD (unique items)
S8         55   (SCALE? ? OR SCALABLE OR SCALING OR SCALABILITY OR PROGRES-
             SIV?)(3N)(ENCOD??? OR COD???) AND (ENCRYPT? OR ENCIPHER? OR E-
             NCYPHER? OR CIPHER? OR CYPHER?)
S9         40   RD (unique items)
S10        20   S9 NOT PY=2002:2005
S11        15   S10 NOT S5
S12       740   AU=(WEE, S? OR WEE S? OR APOSTOLOPOULOS, J? OR APOSTOLOPOU-
             LOS J?)
S13        32   S1:S3 AND S12
S14        14   RD (unique items)
S15        12   S14 NOT (S5 OR S11)
```

5/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

06712762 E.I. No: EIP04068012033
Title: An Overview on Scalable Encryption for Wireless Multimedia Access
Author: Yu, Hong Heather
Conference Title: Internet Quality of Service
Conference Location: Orlando, FL, United States Conference Date: 20030909-20030910
Sponsor: SPIE
E.I. Conference No.: 62209
Source: Proceedings of SPIE - The International Society for Optical Engineering v 5245 2003. p 24-34
Publication Year: 2003
CODEN: PSISDG ISSN: 0277-786X
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 0402W3
Abstract: Wireless environments present many challenges for secure multimedia access, especial streaming media. The availability of varying network bandwidths and diverse receiver device processing powers and storage spaces demand scalable and flexible approaches that are capable of adapting to changing network conditions as well as device capabilities. To meet these requirements, scalable and fine granularity scalable (FGS) compression algorithms were proposed and widely adopted to provide scalable access of multimedia with interoperability between different services and flexible support to receivers with different device capabilities. Encryption is one of the most important security tools to protect content from unauthorized use. If a medium data stream is **encrypted** using non- **scalable** cryptography algorithms, decryption at arbitrary bit rate to provide scalable services can hardly be accomplished. If a medium compressed using **scalable coding** needs to be protected and non-scalable cryptography algorithms are used, the advantages of **scalable coding** may be lost. Therefore **scalable encryption** techniques are needed to provide scalability or to preserve the FGS adaptation capability (if the media stream is FGS coded) and enable intermediate processing of encrypted data without unnecessary decryption. In this paper, we will give an overview of **scalable encryption** schemes and present fine grained **scalable encryption** algorithm. One desirable feature for FGS compatible encryption schemes is to provide simplicity and flexibility in supporting scalable multimedia communication and multimedia content access control in wireless environments. 13 Refs.
Descriptors: *Wireless telecommunication systems; Multimedia systems; Internet; Security of data; Signal processing; Signal encoding; Cryptography; Algorithms
Identifiers: Data streams; Fine granularity scalables (FGS); Wireless network
Classification Codes:
723.5 (Computer Applications); 723.2 (Data Processing); 716.1 (Information & Communication Theory)
716 (Electronic Equipment, Radar, Radio & Television); 723 (Computer Software, Data Handling & Applications)
71 (ELECTRONICS & COMMUNICATION ENGINEERING); 72 (COMPUTERS & DATA PROCESSING)

5/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

06689568 E.I. No: EIP03477743627
Title: Protection of multicast scalable video by secret sharing: Simulation results
Author: Eskicioglu, Ahmet M.; Dexter, Scott; Delp, Edward J.
Corporate Source: Department of Computer Science CUNY Brooklyn College,

Brooklyn, NY 11210, United States
Conference Title: Security and Watermarking of Multimedia Contents V
Conference Location: Santa Clara, CA, United States Conference Date: 20030121-20030124
Sponsor: IS and T; SPIE
E.I. Conference No.: 61509
Source: Proceedings of SPIE - The International Society for Optical Engineering v 5020 2003. p 505-515
Publication Year: 2003
CODEN: PSISDG ISSN: 0277-786X
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical); X; (Experimental)
Journal Announcement: 0401W4
Abstract: Security is an increasingly important attribute for multimedia applications that require prevention of unauthorized access to copyrighted data. Two approaches have been used to protect scalable video content in distribution: Partial **encryption** and **progressive encryption** . Partial **encryption** provides protection for only selected portions of the video. **Progressive encryption** allows **transcoding** with simple packet truncation, and eliminates the need to decrypt the video packets at intermediate network nodes with low complexity. Centralized Key Management with Secret Sharing (CKMSS) is a recent approach in which the group manager assigns unique secret snares to the nodes in the hierarchical key distribution tree. It allows the reconstruction of different keys by communicating different activating shares for the same prepositioned information. Once the group key is established, it is used until a member joins/leaves the multicast group or periodic rekeying occurs. In this paper, we will present simulation results regarding the communication and processing requirements of the CKMSS scheme applied to scalable video. In particular, we have measured the rekey message size and the processing time needed by the server for each join/leave request and periodic rekey event. 26 Refs.
Descriptors: *Multimedia systems; Cryptography; Video signal processing; Security of data; Multicasting; Encoding (symbols); Image compression; Trees (mathematics); Computer simulation
Identifiers: Transcodings
Classification Codes:
723.5 (Computer Applications); 716.4 (Television Systems & Equipment); 723.2 (Data Processing); 921.4 (Combinatorial Mathematics, Includes Graph Theory, Set Theory)
723 (Computer Software, Data Handling & Applications); 716 (Electronic Equipment, Radar, Radio & Television); 717 (Electro-Optical Communication) ; 718 (Telephone & Other Line Communications); 741 (Light, Optics & Optical Devices); 921 (Applied Mathematics)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATION ENGINEERING); 74 (LIGHT & OPTICAL TECHNOLOGY); 92 (ENGINEERING MATHEMATICS)

5/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

06444958 E.I. No: EIP03297543426
Title: Efficient and fully scalable encryption **for MPEG-4 FGS**
Author: Yuan, Chun; Zhu, Bin B.; Wang, Yidong; Li, Shipeng; Zhong, Yuzhuo
Corporate Source: Dept. of Computer Science Tsinghua Univ., Beijing 100084, China
Conference Title: Proceedings of the 2003 IEEE International Symposium on Circuits and Systems
Conference Location: Bangkok, Thailand Conference Date: 20030525-20030528
Sponsor: IEEE Circuits and Systems Society; Mahanakorn University of Technology
E.I. Conference No.: 61136
Source: Proceedings - IEEE International Symposium on Circuits and Systems v 2 2003. p II620-II623 (IEEE cat n 03CH37430)

Publication Year: 2003
CODEN: PICSDI ISSN: 0271-4310
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical); X; (Experimental)
Journal Announcement: 0307W3
Abstract: The newly adopted MPEG-4 Fine Granularity **Scalability** (FGS) video **coding** standard offers full **scalability** to enable easy and flexible adaptation to changing constraints and different requirements. Encryption of an FGS stream should preserve the full scalability. In this paper, we propose a novel and low complexity scheme to encrypt MPEG-4 FGS streams which enables full FGS functionalities. The encrypted FGS stream can be processed by middle stages directly on the ciphertext without decryption. In addition, the proposed scheme has no degradation on either FGS compression efficiency or error resilient performance, and allows random access. Experimental results as well as a preliminary security analysis of the proposed scheme are also included in this paper. 10 Refs.
Descriptors: *Image coding; Cryptography; Image compression; Multimedia systems; Security of data; Error analysis
Identifiers: Scalability analysis
Classification Codes:
723.2 (Data Processing); 723.5 (Computer Applications); 921.6 (Numerical Methods)
723 (Computer Software, Data Handling & Applications); 741 (Light, Optics & Optical Devices); 716 (Electronic Equipment, Radar, Radio & Television); 921 (Applied Mathematics)
72 (COMPUTERS & DATA PROCESSING); 74 (LIGHT & OPTICAL TECHNOLOGY); 71 (ELECTRONICS & COMMUNICATION ENGINEERING); 92 (ENGINEERING MATHEMATICS)

5/5/4 (Item 4 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05960290 E.I. No: EIP01526773077
Title: Secure scalable streaming enabling transcoding **without decryption**
Author: Wee, S.J.; Apostolopoulos, J.G.
Corporate Source: Streaming Media Systems Group Hewlett-Packard Laboratories, Palo Alto, CA, United States
Conference Title: IEEE International Conference on Image Processing (ICIP) 2001
Conference Location: Thessaloniki, Greece Conference Date: 20011007-20011010
Sponsor: IEEE
E.I. Conference No.: 58800
Source: IEEE International Conference on Image Processing v 1 2001. p 437-440 (IEEE cat n 01CH37205)
Publication Year: 2001
CODEN: 85QTAW
Language: English
Document Type: CA; (Conference Article) Treatment: A; (Applications); X ; (Experimental)
Journal Announcement: 0112W5
Abstract: We present a method of secure scalable streaming (SSS) that enables low-complexity and high-quality **transcoding** to be performed at intermediate, possibly untrusted, network nodes without compromising the end-to-end security of the system. SSS **encodes** video into secure **scalable** packets using jointly designed **scalable coding** and **progressive encryption** techniques. This combination allows downstream **transcoders** to perform **transcoding** operations such as bitrate reduction and spatial downsampling by simply truncating or discarding packets, and without decrypting the data. Secure scalable packets have unencrypted headers that can provide hints such as optimal truncation points to downstream **transcoders** . Using these hints, downstream **transcoders** can perform RD-optimal **transcoding** for fine-grain bitrate reduction. The SSS **transcoding** operation has low complexity and is stateless, so SSS **transcoders** can support many simultaneous **transcoding** sessions. SSS

works with existing scalable image and video compression standards and systems including Motion JPEG-2000, 3D subband coding, and MPEG-4 FGS. 11 Refs.

Descriptors: *Image coding; Image communication systems; Security of data ; Cryptography; Computational complexity; Image quality; Packet networks; Client server computer systems; Image compression; Algorithms

Identifiers: Video **transcoding** ; Secure scalable streaming; Video streaming; Decryption; **Scalable coding**

Classification Codes:

723.2 (Data Processing); 723.5 (Computer Applications); 721.1 (Computer Theory (Includes Formal Logic, Automata Theory, Switching Theory & Programming Theory)); 722.4 (Digital Computers & Systems); 723.1 (Computer Programming)

723 (Computer Software, Data Handling & Applications); 721 (Computer Circuits & Logic Elements); 722 (Computer Hardware)

72 (COMPUTERS & DATA PROCESSING)

5/5/5 (Item 5 from file: 8)

DIALOG(R)File 8:Ei Compendex(R)

05915799 E.I. No: EIP01436696575

Title: Secure scalable video streaming for wireless networks

Author: Wee, S.J.; Apostolopoulos, J.G.

Corporate Source: Streaming Media Systems Group Hewlett-Packard Laboratories, Palo Alto, CA, United States

Conference Title: 2001 IEEE Interntional Conference on Acoustics, Speech, and Signal Processing

Conference Location: Salt Lake, UT, United States Conference Date: 20010507-20010511

Sponsor: IEEE

E.I. Conference No.: 58544

Source: ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings v 4 2001. p 2049-2052 (IEEE cat n 01CH37221)

Publication Year: 2001

CODEN: IPRODJ ISSN: 0736-7791

Language: English

Document Type: CA; (Conference Article) Treatment: A; (Applications); T ; (Theoretical)

Journal Announcement: 0110W4

Abstract: We present a wireless video streaming system that securely and efficiently streams video to heterogeneous clients over time-varying communication links. Clients may differ in their display, power, communication, and computational capabilities and wireless channels may have time-varying bandwidths and quality levels that depend on channel usage and channel conditions. End-to-end system efficiency is achieved by placing **transcoders** at intermediate network nodes; these **transcoders** can easily adapt the video stream for particular client capabilities and network conditions. This system uses our proposed method of secure scalable streaming (SSS) to simultaneously achieve scalability, efficiency, and security. Specifically, an SSS coder **encodes** video into secure **scalable** packets by using jointly designed **scalable** video coding, packetization, and **progressive encryption** techniques. This allows downstream SSS **transcoders** to **transcode** the secure scalable packets by simply truncating or eliminating packets, and without decrypting the coded video. A key feature of SSS is that it enables low-complexity **transcoding** operations to be performed at intermediate network nodes without compromising the security of the end-to-end wireless streaming system. 5 Refs.

Descriptors: *Video signal processing; Wireless telecommunication systems ; Packet networks; Telecommunication links; Communication channels (information theory); Image coding; Cryptography; Bandwidth; Security of data; Algorithms

Identifiers: Scalable video streaming; Wireless network; Time-varying communication links; Time-varying bandwidth; End-to-end system; **Transcoder** ; Secure scalable streaming

Classification Codes:
716.4 (Television Systems & Equipment); 716.1 (Information & Communication Theory); 723.5 (Computer Applications); 723.2 (Data Processing); 921.6 (Numerical Methods)
716 (Electronic Equipment, Radar, Radio & Television); 723 (Computer Software, Data Handling & Applications); 921 (Applied Mathematics)
71 (ELECTRONICS & COMMUNICATION ENGINEERING); 72 (COMPUTERS & DATA PROCESSING); 92 (ENGINEERING MATHEMATICS)

5/5/6 (Item 1 from file: 35)

01797421 ORDER NO: AADAA-I9935004
LOW-POWER VLSI ARCHITECTURES FOR FINITE FIELD APPLICATIONS (ERROR CONTROL, CRYPTOGRAPHY)
Author: SONG, LEILEI
Degree: PH.D.
Year: 1999
Corporate Source/Institution: UNIVERSITY OF MINNESOTA (0130)
Adviser: KESHAB K. PARHI
Source: VOLUME 60/06-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 2867. 199 PAGES
Descriptors: ENGINEERING, ELECTRONICS AND ELECTRICAL ; COMPUTER SCIENCE
Descriptor Codes: 0544; 0984

This thesis focuses on the design of VLSI architectures for fundamental finite field arithmetic operations and their applications including Reed-Solomon error-control codecs and elliptic-curve public-key cryptography systems that are extensively used to achieve secure and reliable transmission and storage in digital communication and recording systems.

The basic concepts of finite fields, and the algorithms for RS encoding and decoding, and elliptic curve cryptography are well understood. Previous research in this area addressed design of low-complexity and high-speed dedicated (application-specific) VLSI architectures to cut the cost and meet real-time speed requirements. The work presented in this thesis carries on this design trend for high-speed and low-complexity; moreover, it emphasizes the design of low-energy programmable VLSI architectures for finite field applications.

At the arithmetic units level, various architectures are presented to perform finite field multiplication more efficiently. Low-area and low-latency programmable semi-systolic parallel multiplier, squarer, and exponentiator are proposed. Design of low-complexity dedicated finite field multipliers and dual-basis divider are also presented in this thesis. Moreover, a novel digit-serial multiplication scheme is presented, which has much smaller energy-latency product than the digit-serial multiplier obtained by folding the parallel multiplier.

At the system level, hardware/software codesign is considered for the design of programmable Reed-Solomon **codecs** and energy- **scalable** elliptic curve **encryption** processor. These systems are to be implemented as a combination of hardware and software in application-specific DSP processors with specially designed programmable datapath and dedicated and optimized software to reduce total energy consumption. The cross-talk between hardware and software design ensures that the resulting system best exploited the trade-off between programmability and performance optimization. Energy reduction in RS codecs is achieved by using a novel datapath architecture with low-energy finite field multiplication units; and by reducing the total number of energy-consuming computations through use of a modified RS decoding algorithm and effective software **coding** . The energy- **scalable** elliptic curve **encryption** processor is based on a composite finite field representation, which makes it possible to reduce the total energy consumption by sacrificing some security for low-priority data while adequately protecting the important information.

5/5/7 (Item 1 from file: 65)

DIALOG(R)File 65:Inside Conferences

03435567 INSIDE CONFERENCE ITEM ID: CN036250756
Partial Video Encryption **Based on** Scalable Coding
Kunkelmann, T.; Horn, U.
CONFERENCE: Systems, signals and image processing-International workshop; 5th
INTERNATIONAL WORKSHOP ON SYSTEMS SIGNALS AND IMAGE PROCESSING , 1998; 5TH P: 215-218
University of Zagreb, 1998
ISBN: 9531840105
LANGUAGE: English DOCUMENT TYPE: Conference Papers
CONFERENCE EDITOR(S): Zovko-Cihlar, B.; Grgic, S.; Grgic, M.
CONFERENCE SPONSOR: University of Zagreb
CONFERENCE LOCATION: Zagreb
CONFERENCE DATE: Jun 1998 (199806) (199806)

BRITISH LIBRARY ITEM LOCATION: 4552.205530
NOTE:
Also known as IWSSIP'98
DESCRIPTORS: systems; signals; image processing; IWSSIP

5/5/8 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

8282075 INSPEC Abstract Number: B2005-03-6135C-157, C2005-03-5260D-166
Title: An efficient key scheme for layered access control of MPEG-4 FGS video
Author(s): Zhu, B.B.; Min Feng; Shipeng Li
Author Affiliation: Dept. of Math., Beijing Univ., China
Conference Title: 2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No.04TH8763) Part Vol.1 p.443-6 Vol.1
Publisher: IEEE, Piscataway, NJ, USA
Publication Date: 2004 Country of Publication: USA 3 vol (xxviii+2242) pp.
ISBN: 0 7803 8603 5 Material Identity Number: XX-2004-02548
U.S. Copyright Clearance Center Code: 0-7803-8603-5/04/$20.00
Conference Title: 2004 IEEE International Conference on Multimedia and Expo (ICME)
Conference Date: 27-30 June 2004 Conference Location: Taipei, Taiwan
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: The recently proposed scalable multi-layer FGS (fine granularity **scalability**) **encryption** (SMLFE) **encrypts** an MPEG-4 FGS stream into multiple PSNR and bitrate quality layers for layered access control. Both layer types are supported simultaneously. A simple key scheme was used in SMLFE. In this paper, we propose a novel key scheme for SMLFE that reduces the number of keys maintained and managed by a license server for each protected MPEG-4 FGS stream to two. The new key scheme needs only one key contained in a license to be sent to a consumer. This scheme is based on a cryptographic secure hash function and the Diffie-Hellman key agreement. It satisfies all the requirements of SMLFE and can be used to replace the original simple key scheme for SMLFE. The secure one-way hash and intractability of the Diffie-Hellman and the related problems of computing discrete logarithms ensure the security of the new key scheme. (14 Refs)
Subfile: B C
Descriptors: cryptography; video coding
Identifiers: fine granularity **scalability** **encryption** ; **scalable coding** ; layered access control key scheme; MPEG-4 FGS video; **scalable** multilayer **encryption** ; SMLFE; multiple PSNR layers; multiple bitrate quality layers; key license server; protected MPEG-4 FGS stream; license key; cryptographic secure hash function; Diffie-Hellman key agreement
Class Codes: B6135C (Image and video coding); B6120D (Cryptography); C5260D (Video signal processing); C6130S (Data security)

5/5/10 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

7540700 INSPEC Abstract Number: B2003-04-6220M-002
Title: An integrated approach to encrypting scalable **video**
Author(s): Eskicioglu, A.M.; Delp, E.J.
Author Affiliation: Dept. of Comput. & Inf. Sci., Brooklyn Coll., NY, USA
Conference Title: Proceedings 2002 IEEE International Conference on Multimedia and Expo (Cat. No.02TH8604) Part vol.1 p.573-6 vol.1
Publisher: IEEE, Piscataway, NJ, USA
Publication Date: 2002 Country of Publication: USA 2 vol. (xxx+924+625) pp.
ISBN: 0 7803 7304 9 Material Identity Number: XX-2002-01419
U.S. Copyright Clearance Center Code: 0-7803-7304-9/02/$17.00
Conference Title: Proceedings of IEEE International Conference on Multimedia and Expo (ICME)
Conference Date: 26-29 Aug. 2002 Conference Location: Lausanne, Switzerland
Medium: Also available on CD-ROM in PDF format
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: Scalable video compression is the encoding of a single video stream in multiple layers, each layer with its own bit rate. Because of the computational complexity of full video encryption, partial encryption has emerged as a general trend for both standard and **scalable** video **codecs** . Depending on the application, a particular layer of the video stream is chosen for encryption. In some applications, however, more than one video layer may need to be protected. This results in a more complicated key management as multiple keys are needed. In this paper, we present an integrated approach to encrypting multiple layers. Our proposal is a prepositioned shared secret scheme that enables the reconstruction of different keys by communicating different activating shares for the same prepositioned information. It presents certain advantages over three other key management schemes. (15 Refs)
Subfile: B
Descriptors: code standards; data compression; multimedia communication; public key cryptography; variable rate codes; video codecs; video coding
Identifiers: video compression; video stream; **scalable** video **codecs** ; partial encryption; key management; multiple keys; prepositioned shared secret scheme; key reconstruction; activating shares
Class Codes: B6220M (Speech and video codecs); B6120D (Cryptography); B6135C (Image and video coding); B6210R (Multimedia communications)

5/5/11 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal

16981625 PASCAL No.: 05-0041832
Digital image authentication based on turbo codes
Interactive multimedia and next generation networks : Grenoble, 16-19 November 2004
QING YANG; KEFEI CHEN
ROCA Vincent, ed; ROUSSEAU Franck, ed
Department of Computer Science and Engineering, Shanghai Jiao Tong University, 1954 Huashan Road, Shanghai 200030, China
MIPS 2004 : international workshop on multimedia interactive protocols and systems, 2 (Grenoble FRA) 2004-11-16
Journal: Lecture notes in computer science, 2004, 3311 276-285
ISBN: 3-540-23928-6 ISSN: 0302-9743 Availability: INIST-16343; 354000124390490250
No. of Refs.: 9 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)

Country of Publication: Germany
Language: English
Image ownership authentication is an important part of copyright protection, and digital watermark can be used to implement this task. In this paper, we propose a new image authentication plan concentrating on its security performance. Secret information used as the copyright owner's signature is first turbo **coded** , **encrypted** , **scaled** and then processed in wavelet domain. The original image is also needed in signature extraction. Simulation results are finally given to draw our conclusions.

English Descriptors: Interactive system; Multimedia; Distributed system; Digital image; Authentication; Information use; Cryptography; Digital signature; Turbo code; Copyright; Digital protection; Watermark; Wavelet transformation

French Descriptors: Systeme conversationnel; Multimedia; Systeme reparti; Image numerique; Authentification; Utilisation information; Cryptographie ; Signature electronique; Code Turbo; Droit auteur; Protection numerique; Filigrane; Transformation ondelette

Classification Codes: 001D02B04

5/5/12 (Item 2 from file: 144)
DIALOG(R)File 144:Pascal

16527067 PASCAL No.: 04-0174054
An overview on scalable encryption **for wireless multimedia access Internet quality of service : Orlando FL, 9-10 September 2003**
HONG HEATHER YU
ATIQUZZAMAN Mohammed, ed; HASSAN Mahbub, ed
Panasonic Information and Networking Technologies Laboratory, Unknown
International Society for Optical Engineering, Bellingham WA, United States
Interneet quality of service. Conference (Orlando FL USA) 2003-09-09
Journal: SPIE proceedings series, 2003, 5245 24-34
ISBN: 0-8194-5128-2 ISSN: 1017-2653 Availability: INIST-21760; 354000117819610030
No. of Refs.: 13 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: United States
Language: English
Wireless environments present many challenges for secure multimedia access, especial streaming media. The availability of varying network bandwidths and diverse receiver device processing powers and storage spaces demand scalable and flexible approaches that are capable of adapting to changing network conditions as well as device capabilities. To meet these requirements, scalable and fine granularity scalable (FGS) compression algorithms were proposed and widely adopted to provide scalable access of multimedia with interoperability between different services and flexible support to receivers with different device capabilities. Encryption is one of the most important security tools to protect content from unauthorized use. If a medium data stream is **encrypted** using non- **scalable** cryptography algorithms, decryption at arbitrary bit rate to provide scalable services can hardly be accomplished. If a medium compressed using **scalable coding** needs to be protected and non-scalable cryptography algorithms are used, the advantages of **scalable coding** may be lost. Therefore **scalable encryption** techniques are needed to provide scalability or to preserve the FGS adaptation capability (if the media stream is FGS coded) and enable intermediate processing of encrypted data without unnecessary decryption. In this paper, we will give an overview of **scalable encryption** schemes and present fine grained **scalable encryption** algorithm. One desirable feature for FGS compatible encryption schemes is to provide simplicity and flexibility in supporting scalable

multimedia communication and multimedia content access control in wireless environments.

English Descriptors: Bandwidth; Multimedia; Interoperability; Encryption; Cryptography; Decryption; Wireless network
French Descriptors: Largeur bande; Multimedia; Interoperabilite; Cryptage; Cryptographie; Decryptage; Reseau sans fil

Classification Codes: 001D04A04E

5/5/13 (Item 3 from file: 144)
DIALOG(R)File 144:Pascal

15533522 PASCAL No.: 02-0231727
Load-balancing and scalable multimedia distribution using the Mojette transform
Internet multimedia management systems II
GUEDON Jeanpierre; NORMAND Nicolas; VERBERT Pierre; PARREIN Benoit; AUTRUSSEAU Florent
SMITH John R, ed; PANCHANATHAN Sethuraman, ed; KUO CC Jay, ed; CHINH LE, ed
Image & VideoCommunications team, IRCCyN (UMR 6597), France
International Society for Optical Engineering, Bellingham WA, United States
Internet multimedia management systems. Conference, 2 (Denver CO USA) 2001-08-22
Journal: SPIE proceedings series, 2001, 4519 226-234
ISBN: 0-8194-4243-7 ISSN: 1017-2653 Availability: INIST-21760; 354000097065090230
No. of Refs.: 15 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: United States
Language: English
Video (and other multimedia sources) distribution starts to implement industrial solutions that supposes no quality of service (QoS) properties for the network. To overcome congestion problems in the core of a worldwide Internet network, mirrors sites at the edges of the network are dispatched. Thus the QoS problem is only relevant for the network extremities. Nevertheless, this strategy implies to replicate the multimedia database (denoted as MDB) at multiple edge points to meet the real-time constraints and to establish specific mechanisms between mirror sites to satisfy customer needs as for video distribution. For each or both kind of constraints, we propose a unique data/network representation. The initial information is supposed to be represented as **scalable** (optionally **encrypted**) **encoded** bitstreams. Each bitstream is rearranged into a geometrical buffer. From these data, the Mojette transform projects it onto hyperplanes where each point is called a bin. The two key points for Mojette distributed data are : additional projections can be computed, thus any subset of projections can reconstruct a given buffered flow, an incomplete set of projections can not lead to a partial reconstruction of the source. The first strategy consists in dispatching Mojette MDB (denoted as MMDB) along the network and to use different complementary sites for both the retrieval of the information (when a site is destroyed, other sites can regenerate it) and for its load-balanced distribution (according to the customer location, the nearest neighbor projections coming from different MMDB are used to reconstruct initial data). In this paper, we focus on the mixture of this strategy with the industrial point of view. By replacing each of the mirror site by a set of specific MMDBs, applications like telemedecine or video will gain both specificity (e.g. medical multimedia report of a set of MMDB contain medical information relative to patients located in a given area) and security without sacrificing real-time constraints. Another important feature in this case, is the scalable source description that can be used. Each server of a MMDB set can

contain a high number of projections corresponding to the prime sub-flow to ensure a reconstruction with only one subsidiary projection of any of the other MMDBs of the set. On the contrary, unimportant sub-flows are more distributed on the MMDB set to ensure the global load-balancing property of the network.

English Descriptors: Hyperplane; Buffer system; Telecommunication network; Video technique; Real time; Multimedia databases; Multimedia servers; Internet; Service quality; Load balancing; Scalability; Distributed database

French Descriptors: Hyperplan; Systeme tampon; Reseau telecommunication; Technique video; Temps reel; Base donnee multimedia; Serveur multimedia; Internet; Qualite service; Equilibrage charge; Extensibilite; Base donnee repartie

Classification Codes: 001D04B03; 001D03I01; 001D02B07D

5/5/14 (Item 1 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci

13496336 Genuine Article#: BBL51 Number of References: 9
Title: Digital image authentication based on turbo codes
Author(s): Yang Q (REPRINT) ; Chen KF
Corporate Source: Shanghai Jiao Tong Univ,Dept Comp Sci & Engn,1954 Huashan Rd/Shanghai 200030//Peoples R China/ (REPRINT); Shanghai Jiao Tong Univ,Dept Comp Sci & Engn,Shanghai 200030//Peoples R China/(yangqing@sjtu.edu.cn)
, 2004, V3311, P276-285
ISSN: 0302-9743 Publication date: 20040000
Publisher: SPRINGER-VERLAG BERLIN, HEIDELBERGER PLATZ 3, D-14197 BERLIN, GERMANYINTERACTIVE MULTIMEDIA AND NEXT GENERATION NETWORKS
Series: LECTURE NOTES IN COMPUTER SCIENCE
Language: English Document Type: ARTICLE
Geographic Location: Peoples R China
Journal Subject Category: COMPUTER SCIENCE, THEORY & METHODS
Abstract: Image ownership authentication is an important part of copyright protection, and digital watermark can be used to implement this task. In this paper, we propose a new image authentication plan concentrating on its security performance. Secret information used as the copyright owner's signature is first turbo **coded** , **encrypted** , **scaled** and then processed in wavelet domain. The original image is also needed in signature extraction. Simulation results are finally given to draw our conclusions.
Cited References:
BENEDETTO S, 1998, V16, P231, IEEE J SEL AREA COMM
BERROU C, 1996, V44, P1261, IEEE T COMMUN
CHOU J, 2002, P565, ICME
COX IJ, 1997, V6, P1673, IEEE T IMAGE PROCESS
CVEJIC N, 2003, P217, ICME
DIFFIE W, 1976, V22, P644, IEEE T INFORM THEORY
HAGENAUER J, 1996, V42, P429, IEEE T INFORM THEORY
KURODA K, 2003, DIGITAL WATERMARK US
MALLAT SG, 1989, V37, P2091, IEEE T ACOUST SPEECH

5/5/15 (Item 2 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci

05236113 Genuine Article#: VJ681 Number of References: 9
Title: SECURE PROGRESSIVE TRANSMISSION OF COMPRESSED IMAGES
Author(s): ALJABRI AK; ALASMARI AK
Corporate Source: KING SAUD UNIV,COLL ENGN,EE DEPT,POB

800/RIYADH11421//SAUDI ARABIA/
Journal: IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, 1996, V42, N3 (AUG), P 504-512
ISSN: 0098-3063
Language: ENGLISH Document Type: ARTICLE
Geographic Location: SAUDI ARABIA
Subfile: SciSearch; CC ENGI--Current Contents, Engineering, Technology & Applied Sciences
Journal Subject Category: TELECOMMUNICATIONS; ENGINEERING, ELECTRICAL & ELECTRONIC
Abstract: In most **progressive** image **coding** techniques the compressed data vary in importance for reconstructing the original image. Obtaining certain parts of these data by an eavesdropper could reveal significant information about the transmitted or stored image. In this paper different encryption methods to secure the transmission or storage of such data are proposed and evaluated. The methods are chosen in a manner that allows high encryption and decryption rates, simple key management and utilization of widely available encryption algorithms such as DES (Data Encryption Standard). Effect of channel noise on the encrypted data is also considered and a modification of these methods to combat channel errors is also proposed and evaluated.
Descriptors--Author Keywords: **ENCRYPTION** ; IMAGE COMPRESSION ; **PROGRESSIVE** TRANSMISSION
Research Fronts: 94-2409 001 (CYCLIC CODES; DECODING ALGORITHMS; DELIGNES THEOREM)
94-4771 001 (OPEN DISTRIBUTED SYSTEMS; SIGNATURE SCHEME; NETWORK SECURITY; AUTHENTICATION SERVICE; THRESHOLD CRYPTOSYSTEM; DISCRETE EXPONENTIATION)
Cited References:
AKL SG, 1983, P237, ADV CRYPTOLOGY
ALASMARI AK, 1995, V5, P182, IEEE T CIRC SYST VID
BLAHUT R, 1983, THEORY PRACTICE ERRO
DIFFIE W, 1976, V22, P644, IEEE T INFORM THEORY
GHOSH M, 1995, P10, ERROR CORRECTION SCH
KOU W, 1995, DIGITAL IMAGE COMPRE
MACQ B, 1995, P944, P IEEE JUN
NETRAVALI A, 1995, DIGITAL PICTURES REP
SCHNEIER B, 1996, APPL CRYPTOGRAPHY PR

11/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04530678 E.I. No: EIP96103367924
Title: Secure progressive transmission of compressed images
Author: Jabri, A. Kh. Al; Al-Asmari, A. Kh.
Corporate Source: King Saud Univ, Riyadh, Saudi Arabia
Source: IEEE Transactions on Consumer Electronics v 42 n 3 Aug 1996. p 504-512
Publication Year: 1996
CODEN: ITCEDA ISSN: 0098-3063
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 9612W3
Abstract: In most **progressive** image **coding** techniques the compressed data vary in importance for reconstructing the original image. Obtaining certain parts of these data by an eavesdropper could reveal significant information about the transmitted or stored image. In this paper different **encryption** methods to secure the transmission or storage of such data are proposed and evaluated. The methods are chosen in a manner that allows high **encryption** and decryption rates, simple key management and utilization of widely available **encryption** algorithms such as DES (Data **Encryption** Standard). Effect of channel noise on the **encrypted** data is also considered and a modification of these methods to combat channel errors is also proposed and evaluated. (Author abstract) 9 Refs.
Descriptors: *Security of data; Cryptography; Image communication systems ; Image compression; Data storage equipment; Image coding; Image reconstruction; Algorithms; Spurious signal noise; Communication channels (information theory)
Identifiers: Progressive transmission; Decryption rates; Data **encryption** standard; Channel noise
Classification Codes:
723.2 (Data Processing); 716.1 (Information & Communication Theory); 722.1 (Data Storage, Equipment & Techniques)
723 (Computer Software); 716 (Radar, Radio & TV Electronic Equipment); 722 (Computer Hardware)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS)

11/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04256420 E.I. No: EIP95092862322
Title: Designing a new encryption **method for optimum parallel performance**
Author: Posch, Karl C.; Posch, Reinhard
Corporate Source: Graz Univ of Technology, Graz, Austria
Conference Title: Proceedings of the IEEE 1st International Conference on Algorithms and Architectures for Parallel Processing. Part 2 (of 2)
Conference Location: Brisbane, Aust Conference Date: 19950419-19950421
Sponsor: IEEE
E.I. Conference No.: 43595
Source: IEEE International Conference on Algorithms and Architectures for Parallel Processing v 2 1995. IEEE, Piscataway, NJ, USA,95TH0682-5. p 849-854
Publication Year: 1995
CODEN: 002129
Language: English
Document Type: CA; (Conference Article) Treatment: G; (General Review)
Journal Announcement: 9511W3
Abstract: This paper describes the design process from algorithm design to the chip level for a parallel implementation of a modified version of the RSA **encryption** method. The final system consists of several dozens of custom chips computing modulo exponentiation based on residue number system coding. Emphasis is put on the hierarchical design view, its benefits and its shortcomings. (Author abstract) 15 Refs.

Descriptors: *Cryptography; Parallel processing systems; Algorithms; Software engineering; Integrated circuits; Computational methods; Systems analysis; Hierarchical systems; **Encoding** (symbols); Large **scale** systems
Identifiers: Algorithm design; Modulo exponentiation
Classification Codes:
722.3 (Data Communication, Equipment & Techniques); 723.1 (Computer Programming); 714.2 (Semiconductor Devices & Integrated Circuits); 912.3 (Operations Research); 723.2 (Data Processing)
723 (Computer Software); 722 (Computer Hardware); 714 (Electronic Components); 912 (Industrial Engineering & Management)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS); 91 (ENGINEERING MANAGEMENT)

11/5/4 (Item 1 from file: 65)
DIALOG(R)File 65:Inside Conferences

02539612 INSIDE CONFERENCE ITEM ID: CN026467050
Video Encryption **Based on Data Partitioning and** Scalable Coding **-A Comparison**
Kunkelmann, T.; Horn, U.
CONFERENCE: Interactive distributed multimedia systems and telecommunication services-International workshop; 5th
LECTURE NOTES IN COMPUTER SCIENCE, 1998; NO 1483 P: 95-106
New York, Springer, 1998
ISSN: 0302-9743 ISBN: 3540649557
LANGUAGE: English DOCUMENT TYPE: Conference Papers
CONFERENCE EDITOR(S): Goebel, V.; Plagemann, T.
CONFERENCE LOCATION: Oslo
CONFERENCE DATE: Sep 1998 (199809) (199809)

BRITISH LIBRARY ITEM LOCATION: 5180.185000
DESCRIPTORS: IDMS; multimedia systems; telecommunication services

11/5/8 (Item 3 from file: 144)
DIALOG(R)File 144:Pascal

13992514 PASCAL No.: 99-0177061
Rate-distortion based scalable progressive **image** coding
Mathematics of data/image coding, compression, and encryption : **San Diego CA, 21-22 July 1998**
CAREY W K; VON PISCHKE L A; HEMAMI S S
SCHMALZ Mark S, ed
School of Electrical Engineering, Cornell University, Ithaca, NY 14850, United States
International Society for Optical Engineering, Bellingham WA, United States.
Mathematics of data/image coding, compression, and encryption. Conference (San Diego CA USA) 1998-07-21
Journal: SPIE proceedings series, 1998, 3456 197-208
ISBN: 0-8194-2911-2 ISSN: 1017-2653 Availability: INIST-21760; 354000073149420200
No. of Refs.: 6 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: United States
Language: English
The emergence of distributed, heterogeneous media such as the Internet has established the practical importance of progressive image transmission, in which an image is transmitted in such a way as to admit coarse rendering and recognition at the decoder as early as possible in the bitstream. This paper presents a wavelet-based progressive image transmission algorithm that attempts to achieve several goals not addressed by other image compression algorithms in the literature. First, the algorithm evaluates the tradeoff between rate and distortion as a criterion for selecting wavelet coefficients for transmission. The distortion metric is not limited

to mean squared error; the algorithm provides a framework for investigating any distortion function including psychovisual and segmentation-based distortion metrics. Second, it provides a high degree of spatial scalability by sending coarser resolution information earlier in the bitstream than detail information and does not waste bits by refining high frequency subbands early. Finally, the algorithm is computationally asymmetric, pairing a very fast decoder with an encoder that can be as computationally intensive as required. The performance of the algorithm is comparable with current coders at low bitrates.

English Descriptors: Coding; Decoding circuit; Image processing; Internet; Progressive; Data compression; Image transmission; Segmentation; Wavelet base

French Descriptors: Codage; Circuit decodeur; Traitement image; Internet; Progressif; Compression donnee; Transmission image; Segmentation; Base ondelette